



2049 Century Park East, Suite 2900 Los Angeles, CA 90067 • 310.229.1335

July 13, 2022

Pasha Sternberg
310.229.1335
psternberg@polsinelli.com

VIA E-MAIL (IDTHEFT@OAG.STATE.MD.US)

Office of the Attorney General
Attn: Jeff Karberg, Administrator of the Identity Theft Program
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notification of a Data Security Incident

Dear Mr. Karberg:

We represent Diamond Select Toys & Collectibles, LLC (“Diamond Toys”), 10150 York Road, Cockeysville, Maryland 21030, in connection with an incident that may have involved the personal information of one (1) Maryland resident and are reporting a potential data security incident pursuant to MD. CODE ANN., COM. LAW § 14-3504(h). This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to its submission. While Diamond Toys is notifying you of this incident, Diamond Toys does not waive any rights or defenses relating to the incident or this notice, or the applicability of Maryland law on personal jurisdiction.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

On October 24, 2021, Diamond Toys learned that an unknown third party placed a malicious script on its website. The script was on Diamond Toys’ website from October 23, 2021 through October 25, 2021 and was limited to the checkout page. Upon discovering the incident, Diamond Toys promptly removed the script and investigated with the help of a leading cybersecurity firm. On February 25, 2022, Diamond Toys’ investigation determined that the script could have copied individuals’ names, addresses, transaction details, and payment card information from the checkout page.

NUMBER OF MARYLAND RESIDENTS AFFECTED

Diamond Toys’ investigation determined that one (1) Maryland resident’s personal information may have been involved in the incident. Diamond Toys mailed a notification letter to the individual via USPS mail on July 8, 2022. This notice included a contact number the individual can call should they have questions or require assistance. A copy of the notice sent to the involved individual is enclosed.

polsinelli.com

Atlanta Boston Chicago Dallas Denver Houston Kansas City Los Angeles Nashville New York Phoenix
St. Louis San Francisco Washington, D.C. Wilmington
Polsinelli PC, Polsinelli LLP in California



July 13, 2022

Page 2

STEPS TAKEN RELATING TO THE INCIDENT

Upon learning of the situation, Diamond Toys promptly began an investigation and contained the incident by removing the script from its website. Diamond Toys also hired a leading forensic security firm to further investigate the incident and confirm the security of its website and network. In addition to conducting an investigation into how the incident occurred, Diamond Toys is taking steps to reduce the risk of this type of incident occurring in the future, including reviewing its technical controls. Finally, as discussed above, Diamond Toys notified the individual and provided steps the individual could take to avoid identity theft or fraud, including the tips provided by the FTC on fraud alerts, security and credit freezes.

CONTACT INFORMATION

Please do not hesitate to contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,

Pasha Sternberg

Enclosure



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<MailID>>
<<Name 1>>
<<Address 1>>
<<Address 2>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

RE: NOTICE OF DATA BREACH

Diamond Select Toys & Collectibles, LLC values and respects the privacy of your information, which is why we are writing to advise you of an incident that may have involved some of your personal information.

What Happened? An unknown third party placed computer code that could collect information entered on the checkout page of our website. The code was on our website from approximately October 23, 2021 through October 25, 2021. We removed the computer code and retained a leading forensic security firm to investigate and confirm the security of our computer systems.

What Information Was Involved? After discovering and removing the code, we compiled a list of all transactions that took place during the relevant timeframe. On February 25, 2022, our investigation determined that your name, address, transaction details, and payment card information for your payment card used for order number <<Variable Text Order_ID>> may have been acquired by the third party as a result of the incident.

What We Are Doing. In addition to investigating the incident, we have notified law enforcement and we are taking steps to help prevent a similar incident from occurring in the future, including evaluating additional platforms for educating staff and reviewing technical controls and safeguards. We are not aware of any fraud or misuse of your information as a result of this incident.

What You Can Do. If you detect any suspicious activity on your credit card, you should promptly notify your financial institution or credit card company. You can find more information on steps to protect yourself against identity theft or fraud, including the tips provided by the FTC on fraud alerts, security and credit freezes, and steps you can take to avoid identity theft in the enclosed *Additional Important Information* sheet.

For More Information. For further information and assistance, please call 855-597-1482 from 9:00 A.M. – 9:00 P.M. EST, Monday through Friday.

We value the trust you place in us to protect your privacy and take our responsibility to safeguard your personal information seriously. We apologize for any inconvenience or concern this incident might cause.

Sincerely,

Chuck Terceira
President, Diamond Select Toys & Collectibles, LLC

Additional Important Information

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

The Massachusetts law also allow consumers to place a security freeze on their credit reports. A security freeze can be placed without any charge. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies' online security freeze request procedures:

Equifax Security Freeze

1-888-298-0045

www.equifax.com

P.O. Box 105788

Atlanta, GA 30348

Experian Security Freeze

1-888-397-3742

www.experian.com

P.O. Box 9554

Allen, TX 75013

Trans Union Security Freeze

1-888-909-8872

www.transunion.com

P.O. Box 160

Woodlyn, PA 19094

In order to request a security freeze, you may need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail or, if available, comply with the consumer reporting agencies' online procedures for lifting a security freeze, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at <https://www.annualcreditreport.com/manualRequestForm.action>.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax

1-866-349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian

1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion

1-800-888-4213
www.transunion.com
P.O. Box 1000
Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

This notification was not delayed by law enforcement.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfrp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Iowa Residents: Iowa residents can contact the Office of the Attorney general to obtain information about steps to take to avoid identity theft from the Iowa Attorney General's office at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines IA 50319, 515-281-5164.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, <http://www.marylandattorneygeneral.gov/>.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; <https://ag.ny.gov/consumer-frauds/identity-theft>; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.